Google Patent Search BETA

(hash OR one-way function) seed functional v Search Patents Advanced Patent Sea Google Patent Search

Filing date ○ Return patents filed anytime ◉ Return patents filed between Jan 1948 and Dec 2002

## Patents

Showing: Any status Patents 1 - 14 on (hash OR one-way function) seed functional v

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Secure deterministic encryption key generator system and method

US Pat. 5963646 - Filed Dec 28, 1998 - The PACid Group

As before stated, the bit length of the output of the hash function ... Thus, so long as the secret E-Key seed 50 and the constant value 51 are known, ...

### Memory unit, data processing unit, and data processing method using memory ...

US Pat. 6601140 - Filed Apr 6, 2000 - Sony Corporation

Recorder/player 1 uses the temporary key TMK and the block seed BK SEED in equation ... A one-way Hash function is described in detail in the "Handbook of ...

### Image transformation means including user interface

US Pat. 6476863 - Filed Jul 10, 1998 - Silverbrook Research Pty Ltd

Longevity of Key A general problem of these two protocols is that once the .... The 160-bit seed value for R can be any random number except 0, ...

### Method for seeding a pseudo-random number generator with a cryptographic ...

US Pat. 5732138 - Filed Jan 29, 1996 - Silicon Graphics, Inc.

The graphic hash function, step 110. And from this modified can then be used in forming a password for use in a security which is designated as the "seed," ...

### System and method for generating encryption seed values

US Pat. 7209561 - Filed Sep 20, 2002 - Cybersource Corporation

In step 104, a hash function is applied to produce a hashed 45 value of the ... Thereafter, the selected seed value may be used to generate a key for use in ...

### Printing cartridge with radio frequency identification

US Pat. 6644771 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd

As such, the initial value for R (the random seed) should be programmed ... on MD5 and since the hash result is only 128 bits, HMAC-MD5 is also eliminated. ...

### Printing cartridge with barcode identification

US Pat. 7044589 - Filed Aug 6, 2001

a number of times—N times with a wrong hash value, and expect the result to be 0. ... the choice of one-way function is examined in more detail here. ...

### [APPLICATION] Method and apparatus for camouflaging of data, information and functional ...

US Pat. App 10/015,902 - Filed Oct 30, 2001

The seed derivation function 401 generates a seed value for the key generation ... hash of the PIN, and using this smaller byte sequence as the seed. ...

### Tiered hashing for data access

US Pat. 6516320 - Filed Mar 8, 1999 - Pliant Technologies, Inc.
12B, for example, the dynamic hash pointer component of fixed hash entry 1210 has been adjusted to point to a dynamic hash seed value 1220. ...

Printing cartridge with capacitive sensor identification
US Pat. 6702417 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd
Depending on the one-way function chosen, key generation can be complicated. ... Returns RIE^R], where R is random number based on seed S. Advances R to ...

Method for combining transfer functions with predetermined key creation
US Pat. 6598162 - Filed Mar 24, 1998
The predetermined key is comprised of a transfer function-based mask set to .... be used to encode different information while secure one way hash functions ...

[APPLICATION] Image sensing apparatus including a microcontroller
US Pat. App 9/922,274 - Filed Aug 6, 2001
Given that Protocols 1 and 3 both make use of keyed one-way functions, ... As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Print roll for use in a camera imaging system
US Pat. App 10/309,227 - Filed Dec 4, 2002
Given that Protocols 1 and 3 both make use of keyed one-way functions, ... of silicon implementation (both due to key size and functional implementation). ...

[APPLICATION] Secure handling of stored-value data objects
US Pat. App 10/103,502 - Filed Mar 21, 2002
If the received verification sequence is valid, this proves that the PTD 16 (security.element 20) had the correct seed value. The rapid verification system ...

Google Patent Search BETA

(hash OR verification OR one-way) part share Search Patents Advanced Patent Sea Google Patent Search

Filing date ○ Return patents filed anytime ◉ Return patents filed between Jan 1948 and Dec 2002

Patents Showing: Any status Patents 1 - 20 on (hash OR verification OR one-way) part sharec

Sort by relevance | Sort by date (new first) | Sort by date (old first)

## Method and apparatus for privacy and authentication in wireless networks

US Pat. 5371794 - Filed Nov 2, 1993 - Sun Microsystems, Inc.

The list of supported shared key algorithms is intended to allow for ... is accomplished by encrypting the MD (a non-invertible hash function in the ...

## Transaction processing system

US Pat. 5604802 - Filed Jul 18, 1994 - International Business Machines Corporation

In this embodiment, such shared Key Encrypting Keys, 65 defined to be ... 202 shared with the arbiter A Seal Verification Key 222 enciphered under the ...

## Methods and systems for establishing a shared secret using an authentication ...

US Pat. 6173400 - Filed Jul 31, 1998 - Sun Microsystems, Inc.

If there are no matches between the computed hash and received bits, ... it has the character string or second shared key via a challenge-response (where ...

## Method and apparatus to create encoded digital content

US Pat. 6263313 - Filed Nov 30, 1998 - International Business Machines Corporation

T he recipients of SC(s) can verify the integrity of the SC(s) and its parts by means of the received digital signature and part digests. A one-way hash ...

## Method and apparatus for privacy and authentication in wireless networks

US Pat. RE36946 - Filed Dec 5, 1996 - Sun Microsystems, Inc.

The shared key algorithm will be used to encrypt subsequent data packets. ... is accomplished by encrypting the MD (a non-invertible hash function in the ...

## Secure electronic content management system

US Pat. 6574609 - Filed Sep 14, 1998 - International Business Machines Corporation

The recipients of SC(s) can verify the integrity of the SC(s) and its parts by means of the received digital signature and part digests. A one-way hash ...

## System for tracking end-user electronic content usage

US Pat. 6389538 - Filed Oct 22, 1998 - International Business Machines Corporation

The recipients of SC(s) can verify the integrity of the SC(s) and its parts by means of the received digital signature and part digests. A one-way hash ...

## Cryptographic key exchange using pre-computation

US Pat. 5987131 - Filed Aug 18, 1997 - PictureTel Corporation

2) Each time participants A and B require a shared key: ... Although verification of the signatures on certificates adds to the computational load, ...

## Blind encryption

US Pat. 5638445 - Filed Sep 19, 1995 - Microsoft Corporation
First, it uses the same algorithm to generate a hash 15 information, ... *s
Desirable to encrypt the largest part of the data by means 65 of the shared key ...

## Method and apparatus for stepping pair keys in a key-management scheme

US Pat. 5668877 - Filed Dec 2, 1994 - Sun Microsystems, Inc.
The deso^tion, M=2 thereby providing a one-way function receiving node J uses the
... and this is a shared-key crypto- following representative values of a< ...

## Method and apparatus for interoperable validation of key recovery ...

US Pat. 6058188 - Filed Jul 24, 1997 - International Business Machines Corporation
In this method of key recovery, the verification of the recovery ... as he knows
that Ted published the shared key v, and Ted can therefore calculate k. ...

## Interoperable cryptographic key recovery system with verification by comparison

US Pat. 6052469 - Filed Aug 14, 1998 - International Business Machines Corporation
... on either a SALTO which is a 160-bit random value and some part of the key,
... comprising the steps of: receiving a plurality of shared key recovery ...

## Method and system for authentication and single sign on using ...

US Pat. 6421768 - Filed May 4, 1999 - First Data Corporation
One way to accomplish this registration is to have the first computer 110 ...
Alternatively, the user characteristic and the shared key can be part of a ...

## Auditing login activity in a distributed computing environment

US Pat. 5864665 - Filed Aug 20, 1996 - International Business Machines Corporation
Typically, a one-way hash of the password is used to form the shared key since
the password is an alphanumeric string and the key is usually a number. ...

## Simultaneous electronic transactions with subscriber verification

US Pat. 6141750 - Filed Sep 23, 1997
It may also be convenient to one-way hash strings prior to signing them. ...
to the Post Office separately by means of a different shared key K. This way, ...

## Method and system for determining and maintaining trust in digital data ...

US Pat. 6895507 - Filed Jul 3, 2000 - Time Certain, LLC
The receiver applies the decryption function using the same shared key. ...
A hash function 120 in the signer's software is used to compute a hash result ...

## Software distribution system and software utilization scheme for improving ...

US Pat. 6332025 - Filed Dec 18, 2000 - Kabushiki Kaisha Toshiba
Also, at a time of downloading, a part which is required to be encrypted is
encrypted by the pre-registered shared key. Here, if the download fails in a ...

## Simultaneous electronic transactions

US Pat. 5666420 - Filed Nov 18, 1996
It may also be convenient to one-way hash strings prior her message in any ...
by content of Alice's message). means of a different shared key K. This way, ...

## Method and system for determining and maintaining trust in digital image ...

US Pat. 6948069 - Filed Jul 3, 2000 - Time Certain, LLC
The receiver applies the decryption function using the same shared key. ...

A hash function 120 in the signer's software is used to compute a hash result ...

## Client/server protocol for proving authenticity

US Pat. 6189098 - Filed Mar 16, 2000 - RSA Security Inc.

Moreover, the certificate can include a one way function, such as a cryptographic hash function of a secret value or a root of a hash tree of secret values ...

Stay up to date on these results using the patents RSS feed on (hash OR verification OR one-way) part shared-key part.

Gooooooogle ▶

Result Page: 1 2 3 4 5 6 Next

Google Patent Search BETA

blind access Search Patents Advanced Patent Sea
Google Patent Search

Filing date ○ Return patents filed anytime
◉ Return patents filed between Jan 1948 and Dec 2002

## Patents

Showing: Any status

Patents 1 - 20 on blind access. (0.10 seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Method for providing blind access to an encryption key

US Pat. 5564106 - Filed Mar 9, 1995 - Motorola, Inc.

More generally, there is a need for providing, to a second group, blind access to an encryption key of a predetermined first group member. ...

### Method and system for hierarchical key access and recovery

US Pat. 5917911 - Filed Jan 23, 1997 - Motorola, Inc.

3, the terminal KMC, as part of the blind access protocol, provides a set of encrypted user ID's and the associated encryption keys to the terminal KAC. ...

### Supplemental window and blind unit

US Pat. 4369628 - Filed May 26, 1981 - Wausau Metals Corporation

A window blind 46 is attached to selected surfaces of the sash 36. ... When it is desirable to have access to the original window pane 26 without the ...

### Concentric wrench for blind access opening in a turbine

US Pat. 6321447 - Filed Mar 13, 2000 - General Electric Company

The tubes BACKGROUND OF THE INVENTION are disposed in the blind access opening of the casing and o • j • • ,, , j • • , 20 the flats thereof engage the ...

### Window blind cord winding apparatus

US Pat. 5630456 - Filed May 8, 1996

In the access position window blind cord winding apparatus illustrated in FIG. 1. a user is selectively provided with access to the interior of the spool ...

### Tactile graphics display

US Pat. 5736978 - Filed May 26, 1995 - The United States of America as represented by the Secretary of the Air Force

These publications include the article especially with respect to apparatus for performing specific "Development of Tactile Mice for Blind Access to Comput- ...

### Blind fastener with deformable clamping means

US Pat. 4407619 - Filed May 19, 1980 - Olympic Fastening Systems

This invention relates to so-called blind fasteners for joining side-by-side workpieces, typically two flat sheets to which access is convenient only from ...

### Blind rivet with recessed expanding head

US Pat. 4137817 - Filed Jun 1, 1976 - Olympic Fastening Systems, Inc.

Then, when further movement of the blind-side plate 12 is prevented by the access-side plate 11, the expanding shoulder 29 is pulled into the portion of the ...

## APPARATUS AND METHOD FOR INSTALLING BLIND FASTENERS

US Pat. 3654792 - Filed Jul 25, 1969 - Briles Manufacturing

In view of these and other problems in the art, it is an object thereof where access to one side of a structural joint in dif- jj Most of such blind ...

## Dual-lock blind fastener

US Pat. 5006024 - Filed Mar 5, 1990

Where access to work pieces exists on one side of the Without some locking means, the pin and sleeve may work only, blind fasteners are often used for ...

## Access panel with blind connector

US Pat. 5964617 - Filed Mar 6, 1998 - Whirlpool Corporation

3), the ice maker kit installer removed the access blind connector comprises at least one flexible spreadable improved access panel ...

## Blind orolaryngeal and oroesophageal guiding and aiming device

US Pat. 5339805 - Filed Dec 23, 1992

OTHER PUBLICATIONS Liban, JB et al., A New Blade for Blind Endotracheal ... Herron & Evans [57] ABSTRACT To facilitate rapid, accurate, blind access to the ...

## Hunter's blind

US Pat. 4581837 - Filed Feb 11, 1985

1 and 4, shows the position of the hunter inside of blind 10 when access doors 13 and 14 are closed. In this position the hunter can remain con- 5 cealed in ...

## Bi-directional, anti-reflux vascular access system

US Pat. 4705501 - Filed Apr 12, 1982 - Regents of the University of Minnesota

Separate first access entries 19C and 19D are provided to the respective chambers ... 2 in which the blind chamber 15 is filled with a fluid (usually normal ...

## Blind orolaryngeal and oroesophageal guiding and aiming device

US Pat. 5038766 - Filed Nov 8, 1989

... accurate, blind access to the larynx and/or esophagus such as for emergency intubation of a patient's trachea and simultaneous suctioning of the ...

## Blind and shade cutting center

US Pat. 6604443 - Filed Jul 23, 2001 - Newell Window Furnishings, Inc.

Each release mecha- the access panel 196, the operator loads the stock mini-blind nism 186 includes a spring biased button 188, each having product ...

## System and method for dynamically assigning channels for wireless packet ...

US Pat. 6052594 - Filed Apr 30, 1997 - AT&T Corp.

The higher the latency, the higher the collision probability as more newly selected links are "blind" until communications begin. For packet access ...

## Method and apparatus for pre-identification of keys and switches

US Pat. 5311175 - Filed Nov 1, 1990

With proper treatment, the invention could likewise identify and describe all the keys on the pad, allowing the user full and equally "blind" access to 10 ...

## Implementing force feedback over the World Wide Web and other computer networks

US Pat. 6161126 - Filed Feb 2, 1999 - Immersion Corporation

Perrochon, Louis, et al., "WAB: World Wide Web Access for Blind and Visually ...
Wiker, Steven F. et al., "Development of Tactile Mice for Blind Access to ...

## Blind orolaryngeal and oroesophageal guiding and aiming device

US Pat. 5174283 - Filed May 7, 1992

United States Patent Parker [ii] Patent Number: [45] Date of Patent: [54] BLIND ... accurate, blind access to the larynx or esophagus such as for emergency ...

Stay up to date on these results using the patents RSS feed on blind access.

Gooooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

Google Patent Search beta

blind access key Search Patents Advanced Patent Sea
Google Patent Search

Filing date ○ Return patents filed anytime
● Return patents filed between Jan 1948 and Dec 2002

## Patents

Showing: Any status

Patents 1 - 20 on blind access key. (0.06 seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Method for providing blind access to an encryption key

US Pat. 5564106 - Filed Mar 9, 1995 - Motorola, Inc.

More generally, there is a need for providing, to a second group, blind access to an encryption key of a predetermined first group member. ...

### Method and system for hierarchical key access and recovery

US Pat. 5917911 - Filed Jan 23, 1997 - Motorola, Inc.

As part of the blind access protocol the terminal KAC selects the appropriate encryption key based on the user ID and sends the selected encryption key back ...

### System and method for synchronizing one time pad encryption keys for secure ...

US Pat. 6266413 - Filed May 11, 1999 - Benyamin Ron

No. to Puhl et al. describes a method of providing blind access to an encryption key, such that the key of a first group member is provided to a second ...

### Decryption method and device, and access right authentication method and ...

US Pat. 6275936 - Filed Oct 15, 1998 - Fuji Xerox Co., Ltd.

egates the decryption of the encrypted key by using the blind decryption to the ... To prevent stealing the RSA decryption key from the access ticket, ...

### System and method for synchronizing one time pad encryption keys for secure ...

US Pat. 6445794 - Filed Jun 24, 1998 - Benyamin Ron

A third party could try to guess the identity of the key, in effect copying it ... et al. describes a method of providing blind access to an encryption key, ...

### Method and apparatus for pre-identification of keys and switches

US Pat. 5311175 - Filed Nov 1, 1990

With proper treatment, the invention could likewise identify and describe all the keys on the pad, allowing the user full and equally "blind" access to 10 ...

### MANUALLY OPERABLE TOOL FOR INSTALLING BLIND ANCHOR NUTS

US Pat. 3587271 - Filed Mar 19, 1969 - erpat A

With the shaft 22 of the tool in its first position (in which the key 24 ... a blind anchor nut in situations which have relatively restricted access, ...

### Blind encryption

US Pat. 5638445 - Filed Sep 19, 1995 - Microsoft Corporation

Also attached to this message Private ke£, " cannot ^ access.to *£ ™ the other key is a digital signature that is generated by the certification exchange ...

### Key

US Pat. 4895036 - Filed May 16, 1988 - Supra Products, Inc.
Thus, the key holder 13' is freed and its access key K 50 can be used for its
... Socket 303 is blind, while socket 305 has a hole in the top of the case so ...

## Systems for accessing the internet and geo-defined data and associated methods

US Pat. 6085177 - Filed Sep 16, 1997 - Civic-DDI, LLC
This voice interaction is of beneficial use, particularly to the blind or ...
key 230, for example, the user at the system 210 can access the WWW 214. ...

## Telephonic data access and transmission system

US Pat. 4677659 - Filed Sep 3, 1985
Additionally, in the case of the blind, a braille printer means may be provided
with the key pad unit 14. Appendices A through E form a part of this ...

## Supplemental window and blind unit

US Pat. 4369828 - Filed May 26, 1981 - Wausau Metals Corporation
1, operated by a key 39 that 15 can be removed so as to prevent unauthorized
unlatching. A window blind 46 is attached to selected surfaces of the sash 36. ...

## Car key hole bolt fastening assembly

US Pat. 4121495 - Filed Mar 1, 1976 - ACF Industries, Incorporated
15 Previously blind hole mounting of safety appliances on railways cars has been
done by providing one or more vertically extending key slots in the ...

## Programmable modular connector assembly

US Pat. 4790763 - Filed Sep 15, 1986 - AMP Incorporated
A blind-ended 60 modules are provided with a resilient cantilever latching arm
... 278 of the intersected by a slot 190 formed at the base of access key is ...

## Blind encryption

US Pat. 5761311 - Filed Apr 9, 1997 - Microsoft Corporation
This gives merchant acquirer exchange blob and checks the merchant name contained
40 access to both key k2 and the consumer's credit card within the ...

## Blind encryption

US Pat. 5764768 - Filed Apr 9, 1997 - Microsoft Corporation
This gives merchant acquirer exchange blob and checks the merchant name contained
40 access to both key k2 and the consumer's credit card within the ...

## Remotely operable closure device

US Pat. 6789578 - Filed Apr 30, 2002 - Reflange, Inc.
The segmented clamp 70 locks the blind hub 110 into a fluid-tight seal with the 5
... Once in position, the ROV may access the safety key 150 shown in FIGS. ...

## LOCK ANTI-PICK DEVICE

US Pat. 3765199 - Filed Oct 2, 1972
To this end, the key access to the lock is through the recess 15. ... of other
14 is slightly less than the inner diameter of the in- tools must be "blind". ...

## Intelligent electronic appliance system and method

US Pat. 6850252 - Filed Oct 5, 2000
The meth- 25 ods for key escrow and receiving an escrow certificate are also ...

in such a way that receiving parties can blind the public key and the ...

## Blind unanticipated signature systems

US Pat. 4759064 - Filed Oct 7, 1985

It is of key source 123 is to output a value normally at least where n is the
... Another approach uses algorithmic be checked by anyone with access to the ...

Stay up to date on these results using the patents RSS feed on blind access key.

Gooooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10 Next

Google Patent Search BETA

blind encryption Search Patents Advanced Patent Sea
Google Patent Search

Filing date ○ Return patents filed anytime
● Return patents filed between Jan 1948 and Dec 2002

## Patents

Showing: Any status

Patents 1 - 20 on blind encryption. (0.05 seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Blind encryption
US Pat. 5638445 - Filed Sep 19, 1995 - Microsoft Corporation
However, kl as well as the block public key y; encryption key are encrypted in
... also referred to as the Note that it is necessary to blind the PI key ...

### Blind encryption
US Pat. 5764768 - Filed Apr 9, 1997 - Microsoft Corporation
Thus, to convert me infor- public key y; encryption key are encrypted in ...
mod N. To blind X* examples of such algorithms (eg see Applied Cryptography mod ...

### Blind encryption
US Pat. 5761311 - Filed Apr 9, 1997 - Microsoft Corporation
A novel technique, blinded message; re-encrypting the decrypted, blinded mes-
which we call blind-encryption, is used to protect against ...

### Method for providing blind access to an encryption key
US Pat. 5564106 - Filed Mar 9, 1995 - Motorola, Inc.
More generally, there is a need for providing, to a second group, blind access
to an encryption key of a predetermined first group member. ...

### Electronic watermark system electronic information distribution system and ...
US Pat. 6425081 - Filed Aug 14, 1998 - Canon Kabushiki Kaisha
A description of the blind procedures follows. The encryption systems of the
server and of the user are denoted respectively by El ( ) and E2 ( ), and the ...

### Ideal electronic negotiations
US Pat. 5615269 - Filed Feb 22, 1996
For instance, E^O) may be the encryption, with a trustee's key, ... before it
was Alice who could withhold from Bob the result of their blind negotiation, ...

### System and method for protection of digital works
US Pat. 6885748 - Filed Mar 24, 2000 - ContentGuard Holdings, Inc.
A protocol for blind transformation can be described as follows for the blind
evaluation of the function P(a,x): (i) Cathy encrypts x using her encryption ...

### Public network merchandising system
US Pat. 5825881 - Filed Jun 28, 1996 - Allsoft Distributing Inc.
This "double-blind" method of encryption keeps all information that flows through
the master key server unrecognizable as an added level of security. ...

### Method and system for hierarchical key access and recovery
US Pat. 5917911 - Filed Jan 23, 1997 - Motorola, Inc.

3, the terminal KMC, as part of the blind access protocol, provides a set of encrypted user ID's and the associated encryption keys to the terminal KAC. ...

Decryption method and device, and access right authentication method and ...
US Pat. 6275936 - Filed Oct 15, 1998 - Fuji Xerox Co., Ltd.
The user of the blind decryption device of the present embodiment has the cipher text C, the modulus n and the encryption key E (the second decryption ...

Managing an environment according to environmental preferences retrieved ...
US Pat. 6622115 - Filed Apr 28, 2000 - International Business Machines Corporation
The encryption medium may utilize multiple types of encryption techniques including, but not limited to, double 10 blind encryption is systems, ...

Electronic commerce settlement system
US Pat. 6085168 - Filed Feb 3, 1998 - Fujitsu Limited
According to the first embodiment of the present invention, a blind signature of an ... 4, the transaction management device 5 comprises an encryption key ...

Independent distributed database system
US Pat. 6446092 - Filed Mar 15, 1999 - PeerDirect Company
In the following, two general types of attacks, Blind Attacks and ... If there are encrypted fields, the attacker must know all the encryption keys for the ...

Method and apparatus for implementing electronic cash
US Pat. 4977595 - Filed Mar 28, 1990 - Nippon Telegraph and Telephone Corporation
As the blind signature scheme, for instance, Chaum j proposes in US Pat. No. ... the following blind signature scheme utilizing the RSA encryption scheme. ...

Independent distributed database system
US Pat. 5924094 - Filed Nov 1, 1996 - Current Network Technologies Corporation
The encryption operation 258 requires the initialization vector 260 and a key 262. ... In the following, two general types of attacks, Blind Attacks and ...

Intelligent electronic appliance system and method
US Pat. 6850252 - Filed Oct 5, 2000
Further preferred 30 embodiments provide for rekeying and upgrading of device firmware using a certificate system, and encryption ...

System and method for synchronizing one time pad encryption keys for secure ...
US Pat. 6266413 - Filed May 11, 1999 - Benyamin Ron
No. to Puhl et al. describes a method of providing blind access to an encryption key, such that the key of a first group member is provided to a second ...

[APPLICATION] Signature system presenting user signature information
US Pat. App 9/771,896 - Filed Jan 30, 2001
[0073] Next, the terminal unit 11 encrypts the MD 33 using an encryption key 34, and generates blind information 35. For example, a DBS (data encryption ...

Method for making a blind RSA-signature and apparatus therefor
US Pat. 7058808 - Filed Jun 16, 1999 - Cyphermint, Inc.
The method for making a blind digital RSA-signature according to claim 22, characterized in that the step of RSA-encryption during steps of creating the ...

Absolute public key cryptographic system and method surviving private-key ...
US Pat. 7088821 - Filed May 3, 2001 - Cheman Shaik
1 key equations in this case for Blind-key Encryption are as In Relative Composite-key Algorithm, no blinding is done can be used to further improve the ...

Stay up to date on these results using the patents RSS feed on blind encryption.

Gooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 Next

Google Patent Search BETA

blind encryption hash | Search Patents | Advanced Patent Sea | Google Patent Search

Filing date: ○ Return patents filed anytime ◉ Return patents filed between Jan 1948 and Dec 2002

## Patents

Showing: Any status

Patents 1 - 20 on blind encryption hash. (0.03 seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Blind encryption
US Pat. 5638445 - Filed Sep 19, 1995 - Microsoft Corporation
First, it uses the same algorithm to generate a hash 15 information, ... blob: E[kl]M. After re-encryption of edgment to the merchant either accepting or ...

### Blind encryption
US Pat. 5761311 - Filed Apr 9, 1997 - Microsoft Corporation
Con- nature by using a known algorithm to hash the message into tinuing with the ... After re-encryption of own check on the credit card may then send an ...

### Decryption method and device, and access right authentication method and ...
US Pat. 6275936 - Filed Oct 15, 1998 - Fuji Xerox Co., Ltd.
It is also possible to add a hash function operation unit that performs a ... that inputs a cipher text C' that is blind-effected and an encryption key E; ...

### System and method for protection of digital works
US Pat. 6885748 - Filed Mar 24, 2000 - ContentGuard Holdings, Inc.
In order to perform blind transformation on the individual coordinates of the particular tokens in the document, the first encryption scheme must be an ...

### Independent distributed database system
US Pat. 5924094 - Filed Nov 1, 1996 - Current Network Technologies Corporation
The encryption operation 258 requires the initialization vector 260 and a key ... (a hash of the record's primary key and the stamp field's column name). ...

### Robust and stealthy video watermarking into regions of successive frames
US Pat. 6975743 - Filed Apr 24, 2001 - Microsoft Corporation
Partially and Fully Blind Approaches The exemplary video watermaker may be ... Another example could be cryptographic encryption of these hash values via a ...

### [APPLICATION] Signature system presenting user signature information
US Pat. App 9/771,896 - Filed Jan 30, 2001
The MD function 32 is a unidirectional function such as a hash function, etc. ... the MD 33 using an encryption key 34, and generates blind information 35. ...

### Signature system presenting user signature information
US Pat. 7107454 - Filed Jan 30, 2001 - Fujitsu Limited
The MD function 32 is a unidirectional function such as a hash function, etc. ... the MD 33 using an encryption key 34, and generates blind information 35. ...

### System and method for protection of digital works
US Pat. 7068787 - Filed Mar 24, 2000 - Contentguard Holdings, Inc.

If the digital work is encrypted with a format preserving encryption ... one-way hash function and their corresponding coordinate information is encrypted. ...

### Method for making a blind RSA-signature and apparatus therefor

US Pat. 7058808 - Filed Jun 16, 1999 - Cyphermint, Inc.

When making a blind digital RSA-signature on the initial data M, ... The data F is obtained by RSA-encryption the blinding key R with the help of the ...

### [APPLICATION] Data repository and method for promoting network storage of data

US Pat. App 9/785,535 - Filed Feb 16, 2001

All users with the same family key use the same method to derive the data-item encryption key from the data; users with different family keys use different ...

### [APPLICATION] U.S. Patent 10052464

US Pat. App 10/052,464 - Filed Jan 23, 2002 - Canon Kabushiki Kaisha

[0094] The server 350 includes a contract confirmation unit 302, digital watermarking unit 303, primary encryption unit 304, primary decryption unit 306, ...

### Digital coin tracing using trustee tokens

US Pat. 6446052 - Filed Nov 18, 1998 - RSA Security Inc.

This protocol is unconditionally blind, because the blindness does not rely on ... In two arbitrarily interleaved (and presumed blind) digital signature ...

### Global encryption system

US Pat. 7006633 - Filed Jul 17, 2000 - Global Encryption Standard Corporation

The hash-type function described in the "Alternative Methods" section above ... The use of two trusted intermediaries and blind random numbers inserts an ...

### Auto-recoverable and auto-certifiable cryptosystem with unescrowed signing keys

US Pat. 6122742 - Filed Jun 18, 1997

In an alternative embodiment, the encryption device pre- 25 determines random .... a known public function (eg, applying to it a one-way hash function). ...

### [APPLICATION] Server-assisted regeneration of a strong secret from a weak secret

US Pat. App 9/804,460 - Filed Mar 12, 2001

[0088] This approach can be generalized where the blind function evaluation ... a hash function, or an encryption function, and apply the general methods. ...

### Method for carrying out transactions and device for realizing the same

US Pat. 6859795 - Filed Jul 29, 1999 - Cyphermint, Inc.

To this end, one fixes a cryptographic hash function F which takes values ... N. The RSA system allows several methods of making a blind digital signature. ...

### Network architecture for secure communications between two console-based ...

US Pat. 7031473 - Filed Nov 13, 2001 - Microsoft Corporation

Secure communications may or may not 25 involve encryption, ... Authentication Code — Secure Hash Algorithm 1) operation on them to produce the LAN key 408. ...

### [APPLICATION] U.S. Patent 10183900

US Pat. App 10/183,900 - Filed Jun 26, 2002

In addition, bob uses +1 to "blind" the plaintext value with a random, ... except using a public random hash function (ie, a random oracle) instead of a ...

[APPLICATION] Credential management
US Pat. App 9/757,058 - Filed Jan 8, 2001
The certificate hash is a value that uniquely identifies a certificate. ...
See the "Blind Courier" section below for more info on this. ...

Stay up to date on these results using the patents RSS feed on blind encryption hash.

Google Patent Search BETA

decryption verification value seed value share( Search Patents Advanced Patent Sea Google Patent Search

Filing date ○ Return patents filed anytime ◉ Return patents filed between Jan 1950 and Dec 2002

## Patents

Showing: Any status Patents 1 - 7 on decryption verification value seed value shared

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Method for authenticating a user working in a distributed environment in the ...

US Pat. 5841871 - Filed Nov 18, 1996 - Bull S.A.

... furnishing a verification value called the "seed" and a tally from the ... one-time password received); 50 and further wherein a decryption key of the ...

### Method and apparatus for conducting crypto-ignition processes between thin ...

US Pat. 6263437 - Filed Feb 19, 1998 - Openware Systems Inc

With the random number seed, the client private value is then generated by ... The secret key can be regarded as the valid shared secret key (SSK) and is ...

### Cryptographic key management scheme

US Pat. 6307936 - Filed Sep 16, 1998 - SafeNet, Inc.

Unlike RSA, fixed moduli doesn't provide for a seed and counter but generates p and (p and q, and generator g) can be shared among a community q faster. of ...

### Apparatus and method for implementing IPSEC transforms within an integrated ...

US Pat. 6708273 - Filed Feb 25, 1999 - SafeNet, Inc.

A shared secret key or DEK can later be created by using the other ... by using the values of p and q during the decryption and signing operations of RSA. ...

### Cryptographic co-processor

US Pat. 6704871 - Filed Sep 16, 1998 - SafeNet, Inc.

A shared secret key or DEK can later be created by using the other ... by using the values of p and q during the decryption and signing operations of RSA ...

### System, method, and article of manufacture for secure transactions utilizing ...

US Pat. 6856975 - Filed Mar 30, 2000 - Verify & Protect Inc.

Separately, the payor computer system calculates a final shared value. .... otherwise the decryption of the rolled-over information will yield strange ...

### Auto-Recoverable and Auto-certifiable cryptosystems with RSA or factoring ...

US Pat. 6389136 - Filed Sep 17, 1997

5 is a data flow diagram of the process of private key 1 ... st r-2*r-1 mod n decryption capabilities of a Root Escrow Authority and ...

Stay up to date on these results using the patents RSS feed on decryption verification value seed value shared key.

Google Patent Search BETA

lattice cryptography verification Search Patents Advanced Patent Sea
Google Patent Search

Filing date ○ Return patents filed anytime
● Return patents filed between Jan 1950 and Dec 2002

## Patents

Showing: Any status Patents 1 - 5 on lattice cryptography verification. (0.03 seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Event auditing system

US Pat. 5978475 - Filed Jul 18, 1997 - Counterpane Internet Security, Inc.

An 25 exemplary mutual verification protocol between U0 and Uj is as follows: 1. ... of cryptography; they are described in detail in "Applied Cryptography, ...

### [APPLICATION] Digital signature and authentication method and apparatus

US Pat. App 10/313,082 - Filed Dec 6, 2002 - NTRU Cryptosystems, Incorporated

Verification consists simply of checking that the signature point is in the NTRU ... Schnorr, Segment LLL-Reduction of Lattice Bases, Cryptography and ...

### Secure user identification based on ring homomorphisms

US Pat. 6959085 - Filed May 3, 2000 - NTRU Cryptosystems, Inc.

... "Public-Key Cryptography From Lattice Reduction Problems", In Proc. ... and a verification by the second user, includes the steps: selection by the ...

### Secured signal modification and verification with privacy control

US Pat. 7100050 - Filed May 15, 2000 - International Business Machines Corporation

Public key cryptography allows the authentication agent to authenticate without being able to watermark an image. Watermark information may also be encoded ...

### Digital signature and authentication method and apparatus

US Pat. 7308097 - Filed Dec 6, 2002 - NTRU Cryptosystems, Inc.

The verification procedure is now the same as in the identification scheme. ... Hash functions are used for a variety of purposes in cryptography and other ...

Stay up to date on these results using the patents RSS feed on lattice cryptography verification.

lattice cryptography verification Search Patents

Google Patent Search Help | Advanced Patent Search

Google Patent Search BETA

one-way function seed functional value key Search Patents Advanced Patent Sea Google Patent Search

Filing date ○ Return patents filed anytime ◉ Return patents filed between Jan 1948 and Dec 2002

## Patents

Showing: Any status Patents 1 - 16 on one-way function seed functional value key. (

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Memory unit, data processing unit, and data processing method using memory ...

US Pat. 6601140 - Filed Apr 6, 2000 - Sony Corporation

Recorder/player 1 uses the temporary key TMK and the block seed BK SEED in ...
Here, the one-way function f defines a function from which it is easy to ...

### Image transformation means including user interface

US Pat. 6476863 - Filed Jul 10, 1998 - Silverbrook Research Pty Ltd

Longevity of Key A general problem of these two protocols is that once the ....
The 160-bit seed value for R can be any random number except 0, ...

### Security memory card compatible with secure and non-secure data processing ...

US Pat. 6618789 - Filed Apr 6, 2000 - Sony Corporation

The initial vector INV is an initial value A temporary key TMK may be ...
A one-way Hash function is described in detail in the numeral 10' is a CD and a ...

### Printing cartridge with two dimensional code identification

US Pat. 6416154 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd

Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

### Printing cartridge with radio frequency identification

US Pat. 6644771 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd

Longevity of Key A general problem of these two protocols is that once the ...
As such, the initial value for R (the random seed) should be programmed with ...

### Printing cartridge with barcode identification

US Pat. 7044589 - Filed Aug 6, 2001

Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

### Image sensing apparatus including a microcontroller

US Pat. 6618117 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd

Depending on the one-way function chosen, key generation can be complicated. ...
number based on seed S. Advances R to next in random number sequence. ...

### Prints remaining indicating for camera with variable length print capability

US Pat. 6356715 - Filed Jul 10, 1998 - Silverbrook Research Pty Ltd

Longevity of Key A general problem of these two protocols is that once the ...
As such, the initial value for R (the random seed) should be programmed with ...

### Printing cartridge with capacitive sensor identification

US Pat. 6702417 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd
Depending on the one-way function chosen, key generation can be complicated. ...
Returns RIE^R], where R is random number based on seed S. Advances R to ...

## Method for combining transfer functions with predetermined key creation
US Pat. 6598162 - Filed Mar 24, 1998
The predetermined key is comprised of a transfer function-based mask set to manipulate data at ... in combination with a sufficiently random seed 50 value, ...

## Printing cartridge with a data-carrying integrated circuit device
US Pat. 6953235 - Filed Dec 19, 2002 - Silverbrook Research PTY LTD
15 Longevity of Key A general problem of these two protocols is that once ...
As such, the initial value for R (the random seed) should be programmed with ...

## Shielding manipulations of secret data
US Pat. 7249109 - Filed Mar 2, 2000 - Silverbrook Research Pty Ltd
Protocol 3 requires an additional key (K2), as well as some minimal state machine ... As such, the initial value for R (the random seed) should be pro- ...

[APPLICATION] Printing cartridge with a data-carrying integrated circuit device
US Pat. App 10/322,687 - Filed Dec 19, 2002
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Image sensing apparatus including a microcontroller
US Pat. App 9/922,274 - Filed Aug 6, 2001
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Print roll for use in a camera imaging system
US Pat. App 10/309,227 - Filed Dec 4, 2002
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
of silicon implementation (both due to key size and functional implementation). ...

[APPLICATION] Image printing apparatus including a microcontroller
US Pat. App 9/922,275 - Filed Aug 6, 2001
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

Google Patent Search BETA

one-way function seed value functional value | Search Patents | Advanced Patent Sea | Google Patent Search

Filing date ○ Return patents filed anytime ◉ Return patents filed between Jan 1948 and Dec 2002

## Patents

Showing: Any status | Patents 1 - 20 on one-way function seed value functional value.

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### System with and method of cryptographically protecting communications

US Pat. 6553351 - Filed Dec 30, 1998

... by repeated functional applications of the one-way function starting with ... at least the encoding seed and determines said previous aggregate value as ...

### Image transformation means including user interface

US Pat. 6476863 - Filed Jul 10, 1998 - Silverbrook Research Pty Ltd

Given that Protocols 1 and 30 3 both make use of keyed one-way functions, the choice of ... The 160-bit seed value for R can be any random number except 0, ...

### Memory unit, data processing unit, and data processing method using memory ...

US Pat. 6601140 - Filed Apr 6, 2000 - Sony Corporation

Each block 113 of a part 112 may store a block seed BK-SEED and an initial ... Here, the one-way function f defines a function from which it is easy to ...

### Printing cartridge with two dimensional code identification

US Pat. 6416154 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd

Given that Protocols 1 and 3 both make use of keyed one-way functions, ... As such, the initial value for R (the random seed) should be programmed with a ...

### Printing cartridge with radio frequency identification

US Pat. 6644771 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd

Given that Protocols 1 and 3 both make use of keyed one-way functions, ... As such, the initial value for R (the random seed) should be programmed with a ...

### Security memory card compatible with secure and non-secure data processing ...

US Pat. 6618789 - Filed Apr 6, 2000 - Sony Corporation

BK SEED according to each random number. Further, with the memory card, ... A one-way Hash function is described in detail in the numeral 10' is a CD and a ...

### Printing cartridge with barcode identification

US Pat. 7044589 - Filed Aug 6, 2001

Given that Protocols 1 and 3 both make use of keyed one-way functions, ... As such, the initial value for R (the random seed) should be programmed with a ...

### Method for combining transfer functions with predetermined key creation

US Pat. 6598162 - Filed Mar 24, 1998

The predetermined key is comprised of a transfer function-based mask set to manipulate data at ... in combination with a sufficiently random seed 50 value, ...

### Prints remaining indicating for camera with variable length print capability

US Pat. 6356715 - Filed Jul 10, 1998 - Silverbrook Research Pty Ltd
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

System and method for color dither matrix creation using human-vision-system ...
US Pat. 6862112 - Filed Mar 23, 2001 - Sony Corporation
These functional 60 units may be connected via a system bus 520. ... This may happen even when the pattern giving cost function value 744 is a necessary ...

Printing cartridge with capacitive sensor identification
US Pat. 6702417 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd
Depending on the one-way function chosen, key generation can be complicated. ...
Returns RIE^R], where R is random number based on seed S. Advances R to ...

Image sensing apparatus including a microcontroller
US Pat. 6618117 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd
Depending on the one-way function chosen, key generation can be complicated. ...
number based on seed S. Advances R to next in random number sequence. ...

Printing cartridge with a data-carrying integrated circuit device
US Pat. 6953235 - Filed Dec 19, 2002 - Silverbrook Research PTY LTD
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

Shielding manipulations of secret data
US Pat. 7249109 - Filed Mar 2, 2000 - Silverbrook Research Pty Ltd
Given that Protocols 1 and 3 both make use of keyed one-way functions, the choice of ... As such, the initial value for R (the random seed) should be pro- ...

[APPLICATION] Printing cartridge with a data-carrying integrated circuit device
US Pat. App 10/322,687 - Filed Dec 19, 2002
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Image printing apparatus including a microcontroller
US Pat. App 9/922,275 - Filed Aug 6, 2001
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Image sensing apparatus including a microcontroller
US Pat. App 9/922,274 - Filed Aug 6, 2001
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Print roll for use in a camera imaging system
US Pat. App 10/309,227 - Filed Dec 4, 2002
Given that Protocols 1 and 3 both make use of keyed one-way functions, the choice of one-way function is examined in more detail here. ...

[APPLICATION] Physical and digital secret ballot systems
US Pat. App 9/771,537 - Filed Jan 29, 2001
16, a combination block, functional, and flow diagram for an example audit ...

as by posting the image of the value under a so called "one-way" function or ...

POLYMERIC IMIDO-ESTEES PREPARED FROM MALEIC ADDUCTS OF FATTY ACID ESTERS AND ...

US Pat. 2547498 - Filed Mar 8, 1950 - Rohm a Haas Company

In seed, peanuts, sunflower, linseed, safflower, hemp- addition-, ... reacts with a mono- 25 can be many more groups in each molecule of functional adduct, ...

Stay up to date on these results using the patents RSS feed on one-way function seed value functional value.

Google Patent Search BETA

one-way function seed value functional value I Search Patents Advanced Patent Sea Google Patent Search

Filing date ○ Return patents filed anytime ◉ Return patents filed between Jan 1948 and Dec 2002

## Patents

Showing: Any status Patents 1 - 16 on one-way function seed value functional value

Sort by relevance | Sort by date (new first) | Sort by date (old first)

### Image transformation means including user interface

US Pat. 6476863 - Filed Jul 10, 1998 - Silverbrook Research Pty Ltd

Longevity of Key A general problem of these two protocols is that once the ....
The 160-bit seed value for R can be any random number except 0, ...

### Memory unit, data processing unit, and data processing method using memory ...

US Pat. 6601140 - Filed Apr 6, 2000 - Sony Corporation

Recorder/player 1 uses the temporary key TMK and the block seed BK SEED in ...
Here, the one-way function f defines a function from which it is easy to ...

### Security memory card compatible with secure and non-secure data processing ...

US Pat. 6618789 - Filed Apr 6, 2000 - Sony Corporation

The initial vector INV is an initial value A temporary key TMK may be ...
A one-way Hash function is described in detail in the numeral 10' is a CD and a ...

### Printing cartridge with two dimensional code identification

US Pat. 6416154 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd

Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

### Printing cartridge with radio frequency identification

US Pat. 6644771 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd

Longevity of Key A general problem of these two protocols is that once the ...
As such, the initial value for R (the random seed) should be programmed with ...

### Printing cartridge with barcode identification

US Pat. 7044589 - Filed Aug 6, 2001

Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

### Method for combining transfer functions with predetermined key creation

US Pat. 6598162 - Filed Mar 24, 1998

The predetermined key is comprised of a transfer function-based mask set to manipulate data at ... in combination with a sufficiently random seed 50 value, ...

### Prints remaining indicating for camera with variable length print capability

US Pat. 6356715 - Filed Jul 10, 1998 - Silverbrook Research Pty Ltd

Longevity of Key A general problem of these two protocols is that once the ...
As such, the initial value for R (the random seed) should be programmed with ...

### Image sensing apparatus including a microcontroller

US Pat. 6618117 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd
Depending on the one-way function chosen, key generation can be complicated. ...
number based on seed S. Advances R to next in random number sequence. ...

## Printing cartridge with capacitive sensor identification

US Pat. 6702417 - Filed Aug 6, 2001 - Silverbrook Research Pty Ltd
Depending on the one-way function chosen, key generation can be complicated. ...
Returns RIE^R], where R is random number based on seed S. Advances R to ...

## Printing cartridge with a data-carrying integrated circuit device

US Pat. 6953235 - Filed Dec 19, 2002 - Silverbrook Research PTY LTD
15 Longevity of Key A general problem of these two protocols is that once ...
As such, the initial value for R (the random seed) should be programmed with ...

## Shielding manipulations of secret data

US Pat. 7249109 - Filed Mar 2, 2000 - Silverbrook Research Pty Ltd
Protocol 3 requires an additional key (K2), as well as some minimal state machine
... As such, the initial value for R (the random seed) should be pro- ...

[APPLICATION] Printing cartridge with a data-carrying integrated circuit device
US Pat. App 10/322,687 - Filed Dec 19, 2002
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Image sensing apparatus including a microcontroller
US Pat. App 9/922,274 - Filed Aug 6, 2001
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Image printing apparatus including a microcontroller
US Pat. App 9/922,275 - Filed Aug 6, 2001
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
As such, the initial value for R (the random seed) should be programmed with a ...

[APPLICATION] Print roll for use in a camera imaging system
US Pat. App 10/309,227 - Filed Dec 4, 2002
Given that Protocols 1 and 3 both make use of keyed one-way functions, ...
of silicon implementation (both due to key size and functional implementation). ...

Google Patent Search BETA

two phase key recovery | Search Patents | Advanced Patent Sea | Google Patent Search

Filing date: ○ Return patents filed anytime ● Return patents filed between Jan 1950 and Dec 2002

Patents Showing: Any status

Patents 1 - 10 on two phase key recovery. (0.06 seconds)

Sort by relevance | Sort by date (new first) | Sort by date (old first)

## Two-phase cryptographic key recovery system

US Pat. 5937066 - Filed Oct 2, 1996 - International Business Machines Corporation

Two-Phase Protocol The invention calls for a two-phase system of embedding receiver 104 ("Bob") in country Y by transmitting one or 25 key recovery ...

## Method and apparatus for verifiably providing key recovery information in a ...

US Pat. 5907618 - Filed Jan 3, 1997 - International Business Machines Corporation

's two-phase recovery method, which together further tures ... 3 shows the encryption of a session key using two interactive case, where Alice and Bob ...

## Method and apparatus for interoperable validation of key recovery ...

US Pat. 6058188 - Filed Jul 24, 1997 - International Business Machines Corporation

It is possible to add key recovery functionality to an 5 application that uses a ... 1996, and entitled "Two- Phase Cryptographic Key Recovery System", ...

## Framework-based cryptographic key recovery system

US Pat. 6335972 - Filed Nov 14, 1997 - International Business Machines Corporation

First, there is an optional key recovery registration phase where the parties that desire ... 2.1, two key-recovery-enabled cryptographic applications are ...

## System, method, and computer program for communicating a key recovery block ...

US Pat. 6061454 - Filed Jun 27, 1997 - International Business Machines Corp.

Instead, in et al entitled "TWO-PHASE CRYPTOGRAPHIC KEY Johnson, et al, the information encrypted under the public RECOVERY SYSTEM", Ser. No. ...

## Optimization of commit procedures by utilizing a two-phase commit procedure ...

US Pat. 5261089 - Filed May 16, 1990 - International Business Machines Corporation

4 is a flowchart of recovery processing that is implemented whea an interruption occurs during the two-phase commit procedure described in FIG. 3. FIGS. ...

## Ethernet to phase shift key converter

US Pat. 6556581 - Filed Oct 30, 1998 - Hewlett-Packard Development Company, L.P.

A clock recovery circuit 505 uses the received signal 501 to recover the ... over the two wire medium using a differential phase shift key modulated signal. ...

## Channel equalization system and method

US Pat. 6904110 - Filed May 1, 2001

The non-published or internal partial information about the two key are dynamically changed based on the synchronization parameters such as phase, ...

## Data recovery system

US Pat. 6993537 - Filed Sep 26, 2002 - Lenovo (Singapore) Pte. Ltd.
If an entry was found in the key table and was for an Indoubt delete, ...
a complete UOW (transaction) in a system using the two-phase commit 60 protocol. ...

## Log name exchange for recovery of protected resources

US Pat. 5410684 - Filed Sep 20, 1993 - International Business Machines Corporation
The two-phase commit changes, and the registration information is updated to ...
A key component of this optimization is the Each of these lists has a ...